

Without conceding that Malan U.S. Patent 6,944,673 discloses subject matter that could be properly combined with Messmer and render any of Applicant's claims unpatentable, Applicant contends that Malan is not available to the examiner as a reference.

Malan has a filing date of May 15, 2001, and claims priority to three provisional patent applications each of which has the same filing date of September 8, 2000. However, Applicant's application, which was filed on August 16, 2001, has an effective priority date of **September 7, 2000**, by claiming priority to U.S. Provisional Application Serial No. 60/230,759, filed September 7, 2000, entitled "THWARTING DENIAL OF SERVICE ATTACKS."

The invention claimed in the instant case is fully supported by the specification as filed in Applicant's U.S. Provisional Application Serial No. 60/230,759.

Instant claim 1 is reproduced below. Exemplary support in the Provisional Application for the limitations in claim 1 is shown in **Bold**.

1. A system, [**Provisional Application FIGURES 1-5**] comprising:
 - a control center to coordinate thwarting attacks on a victim data center that is coupled to a network, the control center including: [**Provisional Application Page 7 Line 29 to Page 8 Line 2**]
 - a communication device to receive data from a plurality of monitors, dispersed through the network, with the monitors sending data collected from the network over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from; [**Provisional Application FIGS. 1, 5, Page 8 Lines 3-15**]
 - a computer system, the computer system comprising: [**Provisional Application, Page 7, Lines 1-3; Page 12 Lines 18-20**]
 - a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic [**Provisional Application Page 11, Lines 9-14**]; and

an analysis and filtering process [**Provisional Application Page 3 Lines 19-30**] to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. [**Provisional Application Page 4 Lines 5-18**]

Accordingly, the Malan reference is not available to the examiner in rejection of Applicant's claims under 35 U.S.C. 102 or 103.

Given the prior state of the rejection of these claims over Messmer and Hill and applicant's overcoming of that rejection by incorporation of the subject matter of objected to claim 2 into claim 1, Applicant considers the present claims to be in condition for allowance.

Claims 7-8, 14-16, 24 and 25

The examiner's rejection of claims 7-8, 14-16, 24 and 25 under 35 U.S.C. 103(a) as being unpatentable over Messmer in view of Hill et al, appears illogical given the examiner's use of Messmer in view of Malan et al(6,944,673) in rejecting claims 1, 3, 5-6, 9, 12-13, 18-19, and 21 under 35 U.S.C. 103(a), the base claims to these rejected claims.

Assuming that the examiner meant to reject claims 7-8, 14-16, 24 and 25 in view of Messmer, Malan and Hill, that rejection has been overcome. Moreover, assuming that the examiner maintains a rejection of the base claims, e.g., claim 1 in view of Messmer alone and thus maintains the rejection of e.g., claims 7-8 under Messmer and Hill. Applicant responds that the references fail to suggest much less describe the features of the invention.

In rejection of claim 1, from which claim 7 depends the examiner stated:

As per claims 1, 9, 18, 21, Messmer teaches a central control center(i.e. Counterpane data center) (see lines 26-28) to coordinate thwarting attacks (see lines 1-20), coordinating thwarting attacks is taught in Messmer, because Messmer teaches that the data center monitors network traffic to determine if the customers network is under attack. Messmer teaches a victim data center, because Messmer teaches that outsourcing intrusion detection, one company that does this is Counterpane, Counterpane monitors customers network(see lines 12- 15), the customers network is the victim data center. Messmer teaches a communication device(i.e. probe/black box)(see lines 17-26) to receive data from a plurality of monitors(see lines 23-26), dispersed through the network(see lines 23-27), the monitors sending data collected from the network over a hardened redundant network(see lines 23-28), Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center(see lines 23-

28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network(1 2-26), the central control center has its own network, that is in California or Virginia, where the data from the monitors is collected and sent to the data center (see lines 26-28). Messmer teaches a computer system that includes a process that executes on the computer system to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic(see lines 28-32). Messmer is silent on, an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center. However, Malan et al. discloses analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center(see col. 4, lines 60-65, col. 5, lines 43-53, col. 10, lines 56-65). It would have been obvious to one of ordinary skill in the art at the time of the invention to include Malan's analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center with Messmer, the motivation is that protecting a network from undesirable network traffic is useful which combats denial of service attacks, by having a Dos scrubber can identify malicious traffic, and prevent it from infecting the network(see col. 4, lines 36-65, col. 5, lines 30-53 of Malan et al.)

Applicant contends that Messmer fails to teach at least the feature of a control center to coordinate thwarting attacks on a victim data center According to Messmer, the different products in the article are used to identify attacks, the article says nothing about a control center that coordinates thwarting of attacks. Moreover, the article teaches away from this feature by stating that: "Counterpane staffers advise corporations on how to combat threats but do not make changes to the corporation's equipment."

In addition, Messmer fails to suggest "sending data collected from the network over a redundant network, with the redundant network being a physically separate network from the network that the plurality of monitors collect data from." The examiner contends that this feature is met by Messmer teaching:

Messmer teaches a hardened redundant network because the data collected is sent in encrypted form to the central control center(see lines 23-28). Messmer teaches the redundant network being a physically separate network from the network that the plurality of monitors collect data from, because the plurality of monitors are on the customers network(1 2-26), the central control center has its own network, that is in California or Virginia, where the data from the monitors is collected and sent to the data center (see lines 26-28).

However, claim 1 does not require hardened, and in any event encryption of the data would not necessarily make a network hardened. Claim 1 does require "a redundant network, ...

physically separate network from the network that the plurality of monitors collect data from.” That feature is not met by Messmer having a purported “control center” in California or Virginia, since there is nothing in Messmer's teaching, suggesting that the communication do not traverse at least portions of the network that are under attack.

In addition, Messmer fails to suggest the feature of a process ... to analyze the data from the plurality of monitors to determine network traffic statistics that can identify malicious network traffic. Finally, Messmer fails to suggest, and the examiner acknowledges that Messmer fails to suggest, “an analysis and filtering process to identify malicious traffic and to eliminate the malicious traffic from entering the victim data center.”

Claim 7 adds the limitation that the analysis process classifies attacks and determines a response based on the class of attack. There is nothing in Messmer that suggests an analysis process that determines a response based on the class of attack, which the examiner acknowledges. The examiner relies on Hill for this teaching. However, Hill does not solve any of the deficiencies in Messmer, as noted above.

Applicant's remaining claims are also allowable over the combination of references. . Therefore, for at least the reasons discussed above, these claims are also allowable over this combination of references.

In Applicant's prior response, Applicant argued the distinction of the claims over Mell taken with the other references, as an example of the art cited by Applicant in the IDS that accompanied that Reply. The examiner is invited to review that art again. Applicant maintains that no combination of the art in that IDS, the other art of record or the art applied here renders Applicant's claims anticipated or obvious.

It is believed that all the rejections and/or objections raised by the examiner have been addressed.

Canceled claims, if any, have been canceled without prejudice or disclaimer.

Any circumstance in which the applicant has (a) addressed certain comments of the examiner does not mean that the applicant concedes other comments of the examiner, (b) made arguments for the patentability of some claims does not mean that there are not other good

Applicant : Marinus Frans Kaashoek et al.
Serial No. : 09/931,291
Filed : August 16, 2001
Page : 6 of 6

Attorney's Docket No.: 12221-005001

reasons for patentability of those claims and other claims, or (c) amended or canceled a claim does not mean that the applicant concedes any of the examiner's positions with respect to that claim or other claims.

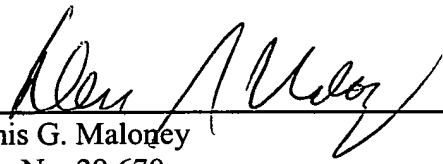
In view of the foregoing remarks, applicant respectfully submits that the application is in condition for allowance and such action is respectfully requested at the examiner's earliest convenience.

No fee is believed due. Please apply any charges to deposit account 06-1050, referencing attorney docket 12221-005001.

Respectfully submitted,

Date: _____

12/14/01



Denis G. Maloney
Reg. No. 29,670

Fish & Richardson P.C.
225 Franklin Street
Boston, MA 02110
Telephone: (617) 542-5070
Facsimile: (617) 542-8906